

vDefend 9.1.1 + Security Services Platform 5.2

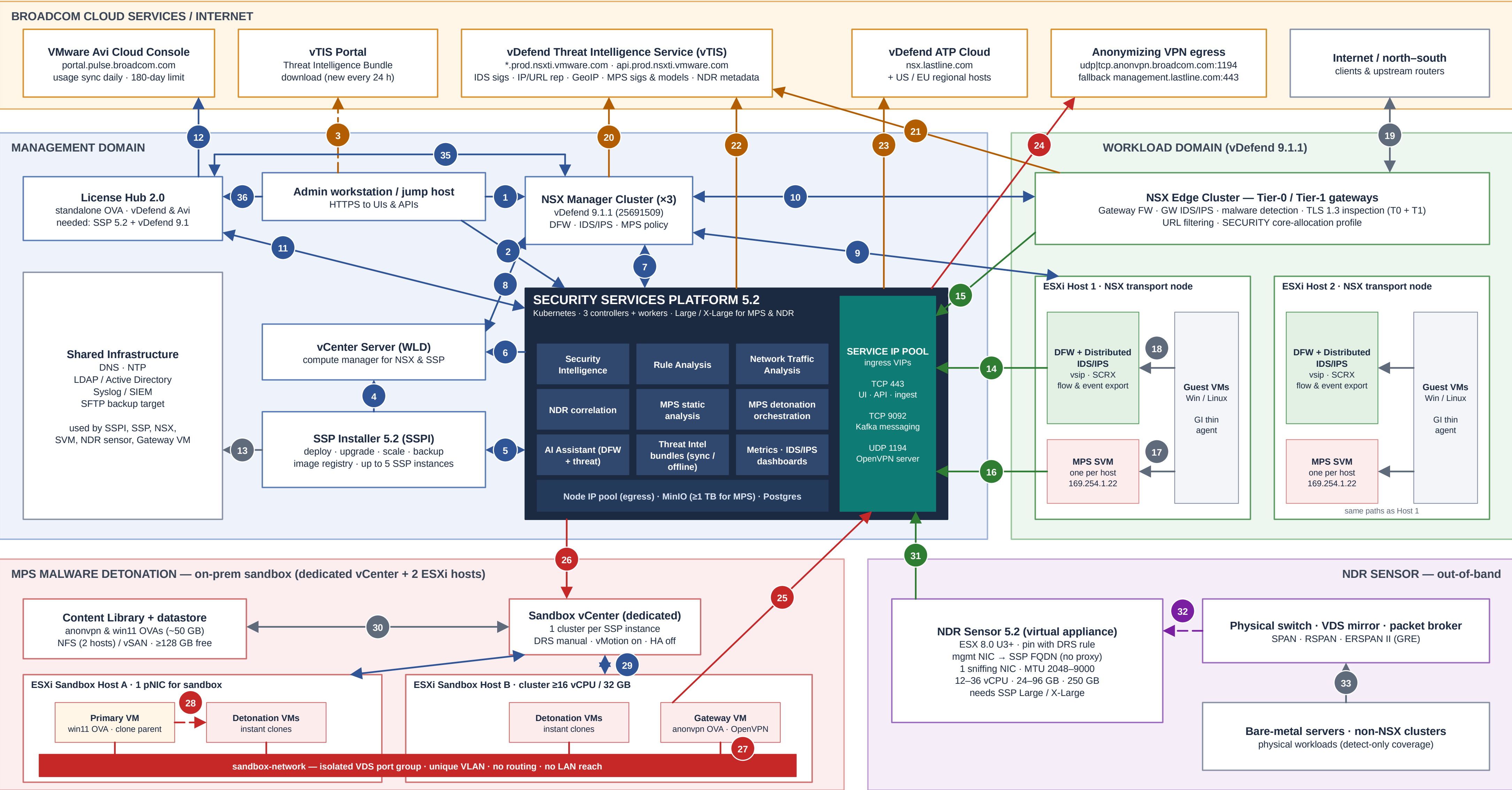
Lateral security, threat prevention and licensing for a VCF 9.1 private cloud

Revised October 14, 2026

License Hub 2.0 paths checked against ports.broadcom.com

Architecture

All components and communication paths · Connected Mode shown, air-gap / manual paths dashed · numbered badges map to the Communication Matrix



Communication Matrix

Numbers match the badges on the architecture drawing; the # cell colour matches the line colour. Mode: All = connected and air-gapped · Connected = needs internet · Air-gap = Disconnected Mode only.

#	Source	Destination	Port / protocol	Purpose / notes	Mode
1	Admin workstation / jump host	NSX Manager cluster (VIP)	TCP 443 (HTTPS)	NSX UI/API — DFW, IDS/IPS and Malware Prevention policy, host preparation	All
2	Admin workstation / jump host	SSP (mgmt FQDN) · SSP Installer UI	TCP 443 (HTTPS)	SSP and SSPI UI/API; upload of the Threat Intelligence Bundle when SSP runs in Disconnected Mode	All
3	Internet-side admin workstation	vTIS Portal	TCP 443 (HTTPS)	Download the Threat Intelligence Bundle (new every 24 h), carry it across the air gap, upload via #2	Air-gap
4	SSP Installer	WLD vCenter · ESXi hosts of the SSP cluster	TCP 443	vCenter API; deploys SSP node VMs (OVF push to hosts)	All
5	SSP Installer ≠ SSP Node IP pool	(both directions)	SSPI → nodes TCP 22 (pre-check), 6443 (K8s API) · nodes → SSPI TCP 443 (registry)	Platform lifecycle: install, upgrade, scale-out, backup/restore	All
6	SSP Node IP pool	WLD vCenter	TCP 443	vSphere CSI — persistent volumes for SSP data services	All
7	SSP ≠ NSX Manager	(both directions)	Node pool → NSX TCP 443 · Service pool → NSX TCP 1234, 1235 · NSX → Service pool TCP 443, 9092	Onboarding and API sync, management/control-plane messaging, Kafka ingest from NSX	All
8	NSX Manager	vCenter Server	TCP 443	Compute manager registration, inventory, cluster preparation	All
9	ESXi transport nodes · MPS SVM	NSX Manager	TN → NSX TCP 1234 (MP), 1235 (CCP), 8080 (repo) · NSX → TN TCP 443 · SVM → NSX TCP 443	Host prep and realization of DFW, IDS/IPS and MPS config; SVM registration (standard NSX ports)	All
10	NSX Edge nodes	NSX Manager	Same ports as #9	Gateway FW, gateway IDS/IPS, TLS inspection and malware-detection configuration	All
11	License Hub 2.0 ≠ SSP	(both directions)	LH → SSP TCP 443 · SSP → LH Service pool 1st IP TCP 443	SSP onboarded as a licensing endpoint (bare-metal security and NDR sensor cores). Needed for SSP 5.2 with vDefend 9.1 / VCF 9.1	All
12	License Hub 2.0	Avi Cloud Console (Broadcom)	TCP 443 — portal.pulse.broadcom.com, prod-cdn-downloads / prod-cdn-uploads.pulse.broadcom.com, access.broadcom.com	Broadcom sign-in, entitlement and license-file download, usage upload (auto, daily retry; must land at least every 180 days). Air-gap: manual file exchange	Connected
13	SSPI, SSP nodes, License Hub (also NSX, SVM, NDR sensor, Gateway VM)	Shared infrastructure services	DNS 53 · NTP UDP 123 · LDAP TCP 389/636 (GC 3268/3269) · Syslog UDP 514 · SFTP TCP 22	Name resolution and time, remote authentication, logs to SIEM, platform and config backups	All
14	ESXi TNs (DFW, distributed IDS/IPS, flow export)	SSP Service IP pool	TCP 443, 9092	Flows → Security Intelligence / NTA, IDS/IPS events, metrics. Hosts must resolve the SSP FQDN	All
15	NSX Edge nodes	SSP Service IP pool	TCP 443, 9092	Gateway IDS/IPS and malware-detection events, extracted files, metrics	All
16	MPS SVM (one per host)	SSP Service IP pool	TCP 443, 9092	Files without a local verdict → on-prem analysis pipeline; verdicts and file events	All
17	Guest VM (GI thin agent)	MPS SVM on the same host	Host-local: SVM 169.254.1.22 ≠ host 169.254.1.2	File extraction and fileless (in-memory script) capture; keep both reserved IPs unused elsewhere	All
18	Guest VM vNIC	DFW / distributed IDS/IPS (kernel)	In-kernel data path (no port)	Inline L2–L7 enforcement and IDS/IPS; SCRX Turbo resizable 4 – 8 vCPU per cluster in 9.1.1	All
19	Internet / north–south clients	NSX Edge (T0 / T1)	Data path	Gateway FW, IDS/IPS, TLS 1.3 inspection (now on T0 and T1), URL filtering, malware detection	All
20	NSX Manager	vTIS	TCP 443 — api.prod.nsx.ti.vmware.com, *prod.nsx.ti.vmware.com	IDS/IPS signature bundles, IP reputation, GeoIP (proxy supported)	Connected
21	NSX Edge (Gateway FW)	vTIS	TCP 443	URL reputation feed for Gateway FW URL filtering	Connected
22	SSP Node IP pool	vTIS	TCP 443 — *.prod.nsx.ti.vmware.com	MPS signatures and ML models, AV signatures, NDR metadata, ATP URL reputation; relayed to NDR sensors	Connected
23	SSP Node IP pool	vDefend ATP Cloud Service	TCP 443 — nsx.lastline.com (+ nsx.west.us / nsx.nl.emea.lastline.com)	Required hosted-backend endpoints; optional opt-in sharing of suspicious files/metadata. Analysis stays on-prem in 5.2	Connected
24	SSP	Anonymizing VPN egress	UDP 1194 udp.anonymvpn.broadcom.com (preferred) · TCP 1194 tcp.anonymvpn... · TCP 443 management.lastline.com	Internet egress for detonation traffic without exposing corporate IPs. Allow-list in proxy; no TLS inspection	Connected
25	Gateway VM (anonymvpn OVA)	SSP Service IP pool	UDP 1194 (OpenVPN)	Tunnel to the VPN server on SSP over the Gateway VM Network (DHCP/static, reaches SSP, ideally no internet)	Connected
26	SSP (MPS detonation orchestration)	Sandbox vCenter (dedicated)	TCP 443	Instant-clones detonation VMs from the Primary VM, lifecycle and cleanup; vCenter administrator account	All
27	Detonation VMs	Gateway VM	L2 on isolated sandbox-network	Dedicated VDS port group, unique VLAN, 1 pNIC per host, no routing — all sample traffic forced into the tunnel	All
28	Primary VM (win11 OVA)	Detonation VMs	Instant clone (vCenter operation)	One clone per suspicious file; runtime behaviour + ML scoring produce the final verdict	All
29	Sandbox vCenter	Sandbox ESXi hosts A / B	TCP 443, 902 · vMotion · NFS TCP 2049 / vSAN	Host management; DRS manual / conservative, vMotion on, HA and Proactive HA off; ≥16 vCPU / 32 GB total	All
30	Sandbox vCenter / hosts	Content Library & datastore	Storage	Local library (~50 GB) with onprem-sandbox anonymvpn · win11 OVAs; NFS (2 hosts) or vSAN (4 hosts), ≥128 GB free	All
31	NDR Sensor (mgmt NIC)	SSP Service IP pool	TCP 443, 9092 — FQDN only, no proxy	Registration, IDS / NTA / SMB events, extracted files; signatures and T1 via SSP (or uploaded bundle)	All
32	Switch SPAN · VDS mirror · packet broker	NDR Sensor sniffing NIC	SPAN · RSPAN · ERSPAN II (GRE, IP 47)	Passive out-of-band copy; one sniffing NIC; MTU 2048–9000 (+50 B for the ERSPAN header)	All
33	Bare-metal and non-NSX workloads	Physical switch	Production traffic	Source of the mirrored traffic NDR inspects (detect-only coverage)	All
34	SSP Installer	registry.k8s.io	TCP 443	SSP lifecycle, per the SSP 5.x Security Hardening Guide (table only — not drawn)	Connected
35	License Hub 2.0 ≠ NSX Manager	(both directions)	LH → NSX TCP 443 · NSX → LH Kafka FQDN TCP 9092 · NSX → LH pool 1st IP TCP 443	vDefend 9.1 licensing for DFW and IDS/IPS: endpoint registration, Kafka config sync, licensing client service and metrics	All
36	Admin workstation / jump host	License Hub 2.0	TCP 443 (UI/API via FQDN, pool 1st IP) · TCP 5480 (appliance mgmt) · TCP 22 (optional SSH)	Onboard NSX, SSP and Avi endpoints; assign licenses; in air-gap mode, carry registration, license and usage files to and from the Avi Cloud Console	All

Sources: Broadcom TechDocs — SSP 5.2 Release Notes (Aug 12 2026), License Hub 2.0 Release Notes & system requirements, MPS prerequisites & malware-analysis pages, NDR Sensor requirements, vTIS overview; vDefend 9.1.1 Release Notes; SSP 5.x Security Hardening Guide. License Hub rows 11, 12, 35, 36 checked against ports.broadcom.com (License Hub for vDefend and Avi 2.0) on Oct 14 2026 — re-confirm all ports there before raising firewall requests.